



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/826,435	04/16/2004	G. Glenn Henry	CNTR.2075	9993
23669 7590 12/11/2007 HUFFMAN LAW GROUP, P.C. 1900 MESA AVE. COLORADO SPRINGS, CO 80906			EXAMINER ZEE, EDWARD	
			ART UNIT	PAPER NUMBER
			2135	
			NOTIFICATION DATE	DELIVERY MODE
			12/11/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTO@HUFFMANLAW.NET

Office Action Summary

Application No.

10/826,435

Applicant(s)

HENRY ET AL.

Examiner

Edward Zee

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 October 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-30 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 11/21/07
- ☒ Interview Summary (PTO-413)
Paper No(s)/Mail Date 20071130
- ☐ Notice of Informal Patent Application
- ☐ Other: _____

DETAILED ACTION

1. This is in response to the amendment filed on October 20th, 2007. Claims 1, 19 and 25 have been amended; Claims 1-30 are pending and have been considered below.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on October 20th, 2007 has been entered.

Claim Rejections - 35 USC § 103

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 1-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yup et al. (2002/0191784) in view of Dhir et al. (2005/0084076) and Yu et al. (7,106,860)..

Claim 1: Yup et al. discloses an apparatus for performing cryptographic operations, comprising:

a. a cryptographic instruction, received by a computing device as part of an instruction flow executing on said computing device, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes that an intermediate result(*data blocks*) be generated [page 3, paragraph 0039];

b. and execution logic(*transformation blocks*), operatively coupled to said cryptographic instruction, configured to execute said one of the cryptographic operations, and configured to generate said intermediate result [page 3, paragraph 0039].

However, Yup et al. does not explicitly disclose performing the instruction on a microprocessor based platform nor performing the instruction within a single microprocessor.

Nonetheless, Dhir et al. discloses a similar apparatus and further discloses performing cryptographic instructions(*ie. program instructions*) to implement the Advanced Encryption Standard algorithm on a microprocessor based platform(*ie. FPGA*) [page 5, paragraph 0051].

Furthermore, Yu et al. discloses a similar apparatus and further discloses performing cryptographic instructions(*ie. executes several steps of an algorithm*) to implement the Advanced Encryption Standard algorithm on single microprocessor(*ie. optimized cipher subprocessor 700*) [column 4, lines 14-39 & figure 7a].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to perform these instructions on a single microprocessor, a microprocessor based platform or any other platform in order to meet particular design requirements.

Claim 2: Yup et al., Dhir et al. and Yu et al. disclose an apparatus as in claim 1 above and Yup et al. further discloses that said one of the cryptographic operations further comprises an

encryption operation, said encryption operation comprising encryption of one or more plaintext blocks(*plurality of channels with input means*) to generate a corresponding one or more ciphertext blocks(*plurality of channels with output means*) [page 2, paragraph 0017].

Claim 3: Yup et al., Dhir et al. and Yu et al. disclose an apparatus as in claim 1 above and Yup et al. further discloses that said one of the cryptographic operations further comprises a decryption operation, said decryption operation comprising decryption of one or more ciphertext blocks(*plurality of channels with input means*) to generate a corresponding one or more plaintext blocks(*plurality of channels with output means*) [page 2, paragraph 0017].

Claims 4-6: Yup et al., Dhir et al. and Yu et al. disclose an apparatus as in claim 1 above and Yup et al. further discloses that said execution logic is configured to interpret an intermediate result field within a control word which is referenced by said cryptographic instruction, wherein the intermediate result field directs said execution logic to generate said intermediate result(*transformations are then repeated on the data block that is fed back until a predetermined number of rounds is completed*) or generate a normal result(*once the predetermined number of rounds are completed, the encrypted data block is fed back to the appropriate storage register*) [page 4, paragraph 0040-0041].

Claims 7-8: Yup et al., Dhir et al. and Yu et al. disclose an apparatus as in claim 1 above and Yup et al. further discloses that said execution logic is configured to interpret a round count field within a control word which is referenced by said cryptographic instruction, wherein the value of said round count field prescribes a number of cipher rounds to be performed on an input block during execution of said one of the cryptographic operations [page 1, paragraph 0004]. The examiner notes that Yup et al. discloses that the apparatus can be operated with a variable

number of rounds, in which the number of rounds is predetermined, thus making it inherent to employ a round count value.

Claim 9: Yup et al., Dhir et al. and Yu et al. disclose an apparatus as in claim 1 above and Yup et al. further discloses that said one of the cryptographic operations is accomplished according to the Advanced Encryption Standard (AES) algorithm [page 2, paragraph 0016].

Claims 11-13: Yup et al., Dhir et al. and Yu et al. disclose an apparatus as in claim 1 above and Yup et al. further discloses that said cryptographic instruction implicitly references one or more registers within said computing device, which include a first register, wherein contents of said first register(*plaintext storage registers*) comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of one or more input text blocks upon which said one of the cryptographic operations is to be accomplished [page 4, paragraph 0043]; and a second register(*cipher block output storage register*), wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding one or more output text blocks, said corresponding one or more output text blocks being generated as a result of accomplishing said one of the cryptographic operations upon one or more input text blocks [page 4, paragraphs 0043-0044].

Claim 15: Yup et al., Dhir et al. and Yu et al. disclose an apparatus as in claim 11 above and Yup et al. further discloses that said one or more registers comprises a fourth register(*cipher key storage register*), wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of

cryptographic key data for use in accomplishing said one of the cryptographic operations [page 3, paragraph 0028].

Claim 16: Yup et al., Dhir et al. and Yu et al. disclose an apparatus as in claim 11 above and Yup et al. further discloses that said one or more registers comprises a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory, said fourth location comprising an initialization vector location, contents of said initialization vector location comprising an initialization vector or initialization vector equivalent for use in accomplishing said one of the cryptographic operations [page 3, paragraph 0027]. The examiner notes that Yup et al. discloses operating the apparatus in CBC mode, which implies the use of initialization vectors. Thus, it is inherent for the initialization vectors to be stored in memory.

Claim 17: Yup et al., Dhir et al. and Yu et al. disclose an apparatus as in claim 11 above and Yup et al. further discloses that said one or more registers comprises a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in memory for access of a control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said one of the cryptographic operations, and wherein said control word comprises an intermediate result field, configured to specify whether a normal result operations(*once the predetermined number of rounds are completed, the encrypted data block is fed back to the appropriate storage register*) or said intermediate result(*transformations are then repeated on the data block that is fed back until a predetermined number of rounds is completed*) is to be generated during execution of said one of the cryptographic [page 4, paragraph 0040-

0041]. The examiner notes that it is inherent for the current round number to be stored in memory if the apparatus is comparing the current round number to a predetermined round number.

Claim 18: Yup et al., Dhir et al. and Yu et al. disclose an apparatus as in claim 1 above and Yup et al. further discloses that said execution logic comprises a cryptography unit, configured execute a plurality of cryptographic rounds on each of one or more input text blocks to generate a corresponding each of one or more output text blocks, wherein said plurality of cryptographic rounds are prescribed by a round count field within a control word that is provided to said cryptography unit [page 3, paragraph 0039-0040].

Claim 19: Yup et al. discloses an apparatus for performing cryptographic operations, comprising:

a. a control word, configured to prescribe that an intermediate result(*data blocks*) be generated during execution of one of the cryptographic(*transformations are then repeated on the data block that is fed back until a predetermined number of rounds is completed*) is to be generated during execution of said one of the cryptographic [page 4, paragraph 0040-0041]. The examiner notes that it is inherent to employ a current round number if the apparatus is comparing the current round number to a predetermined round number;

b. and a cryptography unit(*transformation blocks*) within a device, configured to execute said one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations, wherein said cryptographic instruction also references said control word [page 3, paragraph 0039-0040].

However, Yup et al. does not explicitly disclose performing the instruction on a microprocessor based platform nor performing the instruction within a single microprocessor.

Nonetheless, Dhir et al. discloses a similar apparatus and further discloses performing cryptographic instructions(*ie. program instructions*) to implement the Advanced Encryption Standard algorithm on a microprocessor based platform(*ie. FPGA*) [page 5, paragraph 0051].

Furthermore, Yu et al. discloses a similar apparatus and further discloses performing cryptographic instructions(*ie. executes several steps of an algorithm*) to implement the Advanced Encryption Standard algorithm on single microprocessor(*ie. optimized cipher subprocessor 700*) [column 4, lines 14-39 & figure 7a].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to perform these instructions on a single microprocessor, a microprocessor based platform or any other platform in order to meet particular design requirements.

Claim 20: Yup et al., Dhir et al. and Yu et al. disclose an apparatus as in claim 19 above and Yup et al. further discloses that said control word is stored in memory, and wherein a memory location of said control word is prescribed by contents of a register that is referenced by said cryptographic instruction [page 4, paragraph 0040-0041]. The examiner notes that it is inherent to store the control word in memory because it is being used to determine when the apparatus completes a predetermined number of rounds.

Claim 21: Yup et al., Dhir et al. and Yu et al. disclose an apparatus as in claim 19 above and Yup et al. further discloses that said cryptography unit executes said one of the cryptographic operations according to the Advanced Encryption Standard (AES) algorithm [page 2, paragraph 0016].

Claim 22: Yup et al., Dhir et al. and Yu et al. disclose an apparatus as in claim 19 above and Yup et al. further discloses that said cryptography unit interprets an intermediate result field within said control word to determine whether to generate a normal result(*once the predetermined number of rounds are completed, the encrypted data block is fed back to the appropriate storage register*) or said intermediate result(*transformations are then repeated on the data block that is fed back until a predetermined number of rounds is completed*) [page 4, paragraph 0040-0041].

Claim 23: Yup et al., Dhir et al. and Yu et al. disclose an apparatus as in claim 19 above and Yup et al. further discloses said cryptography unit interprets a round count field within said control word to determine how many block cipher rounds to execute on a block of input text during execution of said one of the cryptographic operations [page 1, paragraph 0004]. The examiner notes that Yup et al. discloses that the apparatus can be operated with a variable

number of rounds, in which the number of rounds is predetermined, thus making it inherent to employ a round count value.

Claim 25: Yup et al. discloses a method for performing cryptographic operations in a device, the method comprising:

a. via a cryptographic instruction, prescribing that an intermediate result be generated during execution of one of a plurality of cryptographic operations(*transformations are then repeated on the data block that is fed back until a predetermined number of rounds is completed*) [page 4, paragraph 0040-0041];

b. and receiving the cryptographic instruction, and generating the intermediate result when executing the one of the cryptographic operations(*transformations are then repeated on the data block that is fed back until a predetermined number of rounds is completed*) [page 4, paragraph 0040-0041].

However, Yup et al. does not explicitly disclose performing the instruction on a microprocessor based platform nor performing the instruction within a single microprocessor.

Nonetheless, Dhir et al. discloses a similar apparatus and further discloses performing cryptographic instructions(*ie. program instructions*) to implement the Advanced Encryption Standard algorithm on a microprocessor based platform(*ie. FPGA*) [page 5, paragraph 0051].

Furthermore, Yu et al. discloses a similar apparatus and further discloses performing cryptographic instructions(*ie. executes several steps of an algorithm*) to implement the Advanced Encryption Standard algorithm on single microprocessor(*ie. optimized cipher subprocessor 700*) [column 4, lines 14-39 & figure 7a].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to perform these instructions on a single microprocessor, a microprocessor based platform or any other platform in order to meet particular design requirements.

Claim 26: Yup et al., Dhir et al. and Yu et al. disclose a method as in claim 25 above and Yup et al. further discloses that said prescribing comprises via a first field within a control word that is referenced by the cryptographic instruction, specifying whether a normal result(*once the predetermined number of rounds are completed, the encrypted data block is fed back to the appropriate storage register*) or the intermediate result(*transformations are then repeated on the data block that is fed back until a predetermined number of rounds is completed*) is to be generated [page 4, paragraph 0040-0041].

Claim 27: Yup et al., Dhir et al. and Yu et al. disclose a method as in claim 25 above and Yup et al. further discloses that said receiving comprises loading the control word from memory [page 4, paragraph 0040-0041]. The examiner notes that it is inherent to store the control word in memory and load it from memory in order to determine when the apparatus completes a predetermined number of rounds.

Claim 28: Yup et al., Dhir et al. and Yu et al. disclose a method as in claim 25 above and Yup et al. further discloses that said receiving comprises executing the one of the cryptographic operations according to the Advanced Encryption Standard (AES) algorithm [page 2, paragraph 0016].

Claim 30: Yup et al., Dhir et al. and Yu et al. disclose a method as in claim 25 above and Yup et al. further discloses that said prescribing comprises via a second field within a control word that is referenced by the cryptographic instruction, specifying how many cipher rounds are to be

executed during execution of the one of the cryptographic operations on a block of input text [page 1, paragraph 0004]. The examiner notes that Yup et al. discloses that the device can be operated with a variable number of rounds, in which the number of rounds is predetermined.

Claims 10, 24 and 29: Yup et al., Dhir et al. and Yu et al. disclose an apparatus as in claims 1, 19 and 22 above, but neither explicitly disclose that said cryptographic instruction is prescribed according to the x86 instruction format. However, it would have been obvious to one of ordinary skill in the art at the time of invention to create the instructions in x86 format or any other format. One would have been motivated to do so in order to conform to the type of platform selected for implementation of the encryption/decryption device.

Claim 14: Yup et al., Dhir et al. and Yu et al. disclose an apparatus as in claim 11 above, but neither explicitly disclose that said one or more registers comprises a third register, wherein contents of said third register indicate a number of text blocks(*channels*) within one or more input text blocks(*plurality of channels*) [page 2, paragraph 0016]. However, it would have been obvious to one of ordinary skill in the art at the time of invention to store the number of blocks being encrypted or decrypted. One would have been motivated to do so in order recognize when the entire encryption or decryption process is complete.

Response to Arguments

5. Applicant's arguments filed October 20th, 2007 have been fully considered but they are not persuasive.

Regarding Claim 1: The Applicant argues that Yup et al. does not disclose cryptographic instructions. However, the Examiner respectfully disagrees and submits that while the exact

term “cryptographic instructions” is not disclosed, Yup et al. does in fact teach cryptographic instructions(*ie. finite state machine controllers which controls the operation of the remaining portions of the circuit*) [page 3, paragraph 0025].

Furthermore, the Applicant argues that Yup et al. nor Dhir et al. disclose performing cryptographic operations/instructions within a single microprocessor. However, the Examiner submits that this is moot in view of the new ground of rejection.

Moreover, the Applicant argues that Yup et al. does not disclose execution logic coupled to a cryptographic instruction, configured to generate and intermediate result. However, the Examiner respectfully disagrees and submits that Yup et al. does disclose an instruction to generate intermediate results(*ie. under control of a START control signal....this cycle continues until the data block has been transformed a predetermined number of rounds, thus each round can be viewed as an “intermediate result”*) [page 4, paragraph 0040].

Additionally, the Applicant argues that Yup et al. does not disclose a data block coupled to a cryptographic instruction. However, the Examiner respectfully disagrees and submits that Yup et al. does disclose this feature(*ie. finite state machine controllers which controls the operation of the remaining portions of the circuit, such as the data blocks*) [page 3, paragraphs 0025 & 0039].

Regarding Claim 19: The Applicant’s remarks regarding this claim have been discussed in Claim 1 above.

Regarding Claim 25: The Applicant’s remarks regarding this claim have been discussed in Claims 1 and 19 above.

Conclusion

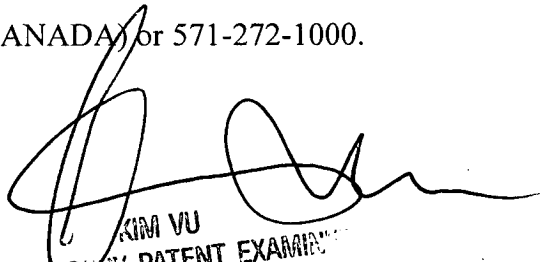
6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Denjanenko et al. (2004/0202317) discloses an Advanced Encryption Standard (AES) implementation as an instruction set extension..

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edward Zee whose telephone number is (571) 270-1686. The examiner can normally be reached on Monday through Thursday 9:00AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ
November 30, 2007


KIM VU
SENIOR PATENT EXAMINER
TECHNICAL CENTER 2100